

Firepower Threat Defense TCP 연결 플래그 해석 (연결 빌드업 및 해체)

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[TCP 연결 문제 해결](#)

[FTD TCP 연결 플래그](#)

[TCP 연결 플래그 값](#)

소개

이 문서에서는 FTD(Firepower Threat Defense)를 통해 TCP 연결을 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- TCP 통신 프로토콜에 대한 기본 지식.
- FTD CLI에 대한 기본 지식

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

TCP 연결 문제 해결

FTD를 통해 TCP 연결을 트러블슈팅할 때 각 연결에 대해 표시되는 연결 플래그는 FTD를 통한 TCP 연결 상태에 대한 풍부한 정보를 제공합니다. 이 정보는 FTD와 관련된 문제 및 네트워크의 다른 위치에서 발생하는 문제를 트러블슈팅하는 데 사용할 수 있습니다.

Disclaimer: The information in this document was created based on FTD devices on version 7.0 in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

모든 FTD 인터페이스의 보안 레벨은 00이므로 show conn 출력은 인터페이스 번호를 기반으로 합니다. 특히 VPIF(Virtual Platform Interface Number)가 더 높은 인터페이스가 먼저 표시됩니다.

Disclaimer : The **show conn** output can be too long, hence it is recommended to use 'terminal pager' or write into a file saved in disk0: such as 'show conn | redirect filename.txt'

```
firepower# show conn
3 in use, 22 most used
Inspect Snort:
preserve-connection: 3 enabled, 0 in effect, 22 most enabled, 0 most in effect

TCP ISP2 192.168.50.14:35518 Inside 192.168.45.130:22, idle 0:10:00, bytes 7164, flags UIO N1
TCP ISP2 192.168.50.14:80 Inside 192.168.45.130:54554, idle 0:00:13, bytes 0, flags U N1
TCP Inside 192.168.45.130:34070 ISP1 10.31.104.78:3128, idle 0:00:02, bytes 1187822, flags UIO N1
```

의 출력에서 인터페이스 VPIF 값을 확인할 수 있습니다. show interface detail 명령을 실행합니다.

```
firepower# show interface detail | i Interface number is|Interface
Interface GigabitEthernet0/0 "ISP1", is up, line protocol is up
Control Point Interface States:
  Interface number is 3
Interface config status is active
Interface state is active
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
Control Point Interface States:
  Interface number is 4
Interface config status is active
Interface state is active
Interface GigabitEthernet0/2 "DMZ", is up, line protocol is up
Control Point Interface States:
  Interface number is 5
Interface config status is active
Interface state is active
Interface GigabitEthernet0/3 "ISP2", is up, line protocol is up
Control Point Interface States:
  Interface number is 6
Interface config status is active
Interface state is active
```

이 show conn long 및 show conn detail 명령은 연결의 Initiator 및 Responder에 대한 세부 정보를 제공합니다.

```
firepower# show conn long
3 in use, 22 most used
Inspect Snort:
preserve-connection: 3 enabled, 0 in effect, 22 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
B - TCP probe for server certificate,
b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - initiator FIN, f - responder FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
```

n - GUP, O - responder data, o - offloaded,
P - inside back connection, p - passenger flow
q - SQL*Net data, R - initiator acknowledged FIN,
R - UDP SUNRPC, r - responder acknowledged FIN,
T - SIP, t - SIP transient, U - up,
V - VPN orphan, v - M3UA W - WAAS,
w - secondary domain backup,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow

TCP ISP2: 192.168.50.14/35518 (192.168.50.14/35518) Inside: 192.168.45.130/22
(192.168.45.130/22), flags UIO N1, idle 9m13s, uptime 9m17s, timeout 1h0m, bytes 7164

Initiator: 192.168.50.14, Responder: 192.168.45.130

Connection lookup keyid: 168317598

TCP ISP2: 192.168.50.14/80 (192.168.50.14/80) Inside: 192.168.45.130/54554
(192.168.45.130/54554), flags U N1, idle 0s, uptime 10s, timeout 1h0m, bytes 0

Initiator: 192.168.45.130, Responder: 192.168.50.14

Connection lookup keyid: 168367034

TCP Inside: 192.168.45.130/34070 (192.168.45.130/34070) ISP1: 10.31.104.78/3128
(10.31.104.78/3128), flags UIO N1, idle 0s, uptime 46s, timeout 1h0m, bytes 617331

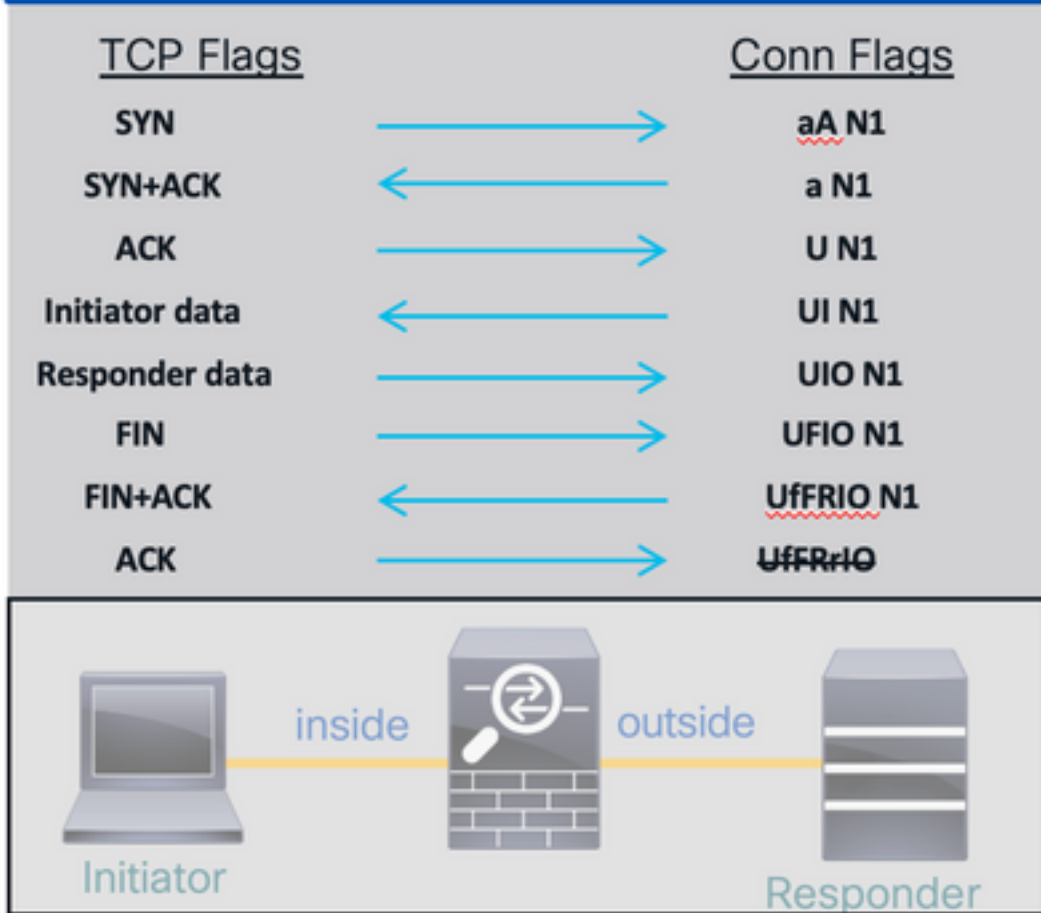
Initiator: 192.168.45.130, Responder: 10.31.104.78

Connection lookup keyid: 168227654

FTD TCP 연결 플래그

이 표에서는 TCP 상태 머신의 여러 단계에 있는 FTD TCP 연결 플래그를 보여줍니다. FTD에서는 보안 수준이 항상 '0'이므로 인바운드 연결과 아웃바운드 연결에 대해 연결 플래그가 동일합니다. 이러한 플래그는 FTD에서 show conn 명령을 사용하여 볼 수 있습니다.

TCP Connection



TCP 연결 플래그 값

이 표에서는 패킷 수신 시 제거되고 추가되는 TCP 연결 플래그를 보여줍니다.

Flags REMOVED upon Receipt of Packet	Flag	Description
[REMOVED]	a	Awaiting Initiator ACK to SYN
	A	Awaiting Responder ACK to SYN
[ADDED]	U	Up - 3-way Handshake Complete
	I	Received Initiator Data
	O	Received Responder Data
	F	Received Initiator FIN
	f	Received Responder FIN
	R	Received Initiator ACK to FIN
	N1	Inspected by Snort with preserve-connection enabled
	N2	Inspected by Snort with preserve-connection in effect

연결에서 가능한 모든 플래그를 보려면 `show conn detail` 명령을 사용합니다.

firepower# **show conn detail**

1 in use, 22 most used

Inspect Snort:

preserve-connection: 1 enabled, 0 in effect, 22 most enabled, 0 most in effect

Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,

B - TCP probe for server certificate,

b - TCP state-bypass or nailed,

C - CTIQBE media, c - cluster centralized,

D - DNS, d - dump, E - outside back connection, e - semi-distributed,

F - initiator FIN, f - responder FIN,

G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,

i - incomplete, J - GTP, j - GTP data, K - GTP t3-response

k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media

N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)

n - GUP, O - responder data, o - offloaded,

P - inside back connection, p - passenger flow

q - SQL*Net data, R - initiator acknowledged FIN,

R - UDP SUNRPC, r - responder acknowledged FIN,

T - SIP, t - SIP transient, U - up,

V - VPN orphan, v - M3UA W - WAAS,

w - secondary domain backup,

X - inspected by service module,

x - per session, Y - director stub flow, y - backup stub flow,

Z - Scansafe redirection, z - forwarding stub flow

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.